have not been used in a previous protocol run between the user device and the bootstrapping server.

11. An apparatus, comprising:

one or more processors; and

one or more memories including computer program code, the one or more memories and the computer program code configured, with the one or more processors, to cause the apparatus to perform at least the following:

a) receive, at a user device, a random number from a bootstrapping server;

b) generate a digest authentication response based on the random number and a password;

c) send the digest authentication response to the bootstrapping server;

d) receive a successful authentication response from the bootstrapping server;

e) derive a shared key between the user device and the bootstrapping function, wherein the digest authentication response is based on a password, and deriving the shared key is based on the digest authentication response and the password.

12. The apparatus according to claim **11**, wherein the apparatus is further caused to negotiate, at the user device, an authenticated transaction layer security session before receiving the random number.

13. The apparatus according to claim **11**, wherein the digest authentication response is based on a key derivation function using the password and a digest response parameter as input values

14. The apparatus according to claim **12**, where the digest response parameter is calculated using a hash function which uses a nonce as an input.

15. The apparatus according to claim **11**, where the digest response parameter is modified by applying a hash function to a user name, the password, and a nonce value.

16. The apparatus according to claim **11**, where the digest response parameter is modified by applying a hash function to the digest response parameter and the password.

17. The apparatus according to claim **11**, where the shared key is generated by applying a hash function to at least one fresh parameter and an arbitrary string parameter.

18. The apparatus according to claim **14**, where the hash function is a key derivation function used in a generic bootstrapping architecture.

19. A generic bootstrapping architecture method, the method comprising:

a) receiving, at a user device, a random number from a bootstrapping server;

b) generating a digest authentication response based on the random number and a password;

c) sending the digest authentication response to the bootstrapping server;

d) receiving a successful authentication response from the bootstrapping server; and

e) deriving a shared key between the user device and the bootstrapping function, wherein the digest authentication response is based on a password, and deriving the shared key is based on the digest authentication response and the password.

20. A computer program product stored on a non-transitory computer readable medium and comprising:

code for producing the steps of:

a) receiving, at a user device, a random number from a bootstrapping server;

b) generating a digest authentication response based on the random number and a password;

c) sending the digest authentication response to the bootstrapping server;

d) receiving a successful authentication response from the bootstrapping server; and

e) deriving a shared key between the user device and the bootstrapping function, wherein the digest authentication response is based on a password, and deriving the shared key is based on the digest authentication response and the password.

* * * * *